


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

IPSEC and cache and entries and DNS and server and domain



THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Terms used

IPSEC and cache and entries and DNS and server and domain and name

Found 33,855 of 203,282

Sort results by

 relevance ☒
☒ [Save results to a Binder](#)

 Try an [Advanced Search](#)

Display results

 expanded form ☒
☒ [Search Tips](#)

 Try this search in [The ACM Guide](#)
☐ Open results in a new window

Results 1 - 20 of 200

 Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

 Relevance scale ☐ ☐ ☐ ☐ ☐

### 1 [A public-key based secure mobile IP](#)

 John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent  
 October 1999 **Wireless Networks**, Volume 5 Issue 5

Publisher: Kluwer Academic Publishers

 Full text available: [pdf\(255.65 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

### 2 [A self-configuring and self-administering name system with dynamic address assignment](#)

 February 2002 **ACM Transactions on Internet Technology (TOIT)**, Volume 2 Issue 1

Publisher: ACM Press

 Full text available: [pdf\(908.57 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

In this article we present a distributed system that stores name-to-address bindings and provides name resolution to a network of computers. This name system consists of a network of name services that are individually self-configuring and self-administering. The name service consists of an agent program that works in conjunction with the current implementation of the Domain Name System (DNS) program. The DNS agent program automatically configures the Berkeley Internet Name Domain (BIND) process ...

**Keywords:** Berkeley Internet Name Domain, dynamic reconfiguration, name-to-name address binding, self-administering systems, self-configuring systems

### 3 [Mobile Code and Distributed Systems: A new approach to DNS security \(DNSSEC\)](#)

Giuseppe Ateniese, Stefan Mangard

 November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**

Publisher: ACM Press

 Full text available: [pdf\(600.56 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The Domain Name System (DNS) is a distributed database that allows convenient storing and retrieving of resource records. DNS has been extended to provide security services (DNSSEC) mainly through public-key cryptography. We propose a new approach to

DNSSEC that may result in a significantly more efficient protocol. We introduce a new strategy to build chains of trust from root servers to authoritative servers. The techniques we employ are based on symmetric-key cryptography.

**Keywords:** authentication protocols, digital signatures, domain name system security (DNSSEC), symmetric encryption

#### 4 A public-key based secure mobile IP



John Zao, Stephen Kent, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra

September 1997 **Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking MobiCom '97**

**Publisher:** ACM Press

Full text available: [pdf\(1.95 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#)

#### 5 An end-to-end approach to host mobility



Alex C. Snoeren, Hari Balakrishnan

August 2000 **Proceedings of the 6th annual international conference on Mobile computing and networking MobiCom '00**

**Publisher:** ACM Press

Full text available: [pdf\(1.35 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We present the design and implementation of an end-to-end architecture for Internet host mobility using dynamic updates to the Domain Name System (DNS) to track host location. Existing TCP connections are retained using secure and efficient connection migration, enabling established connections to seamlessly negotiate a change in endpoint IP addresses without the need for a third party. Our architecture is secure—name updates are effected via the secure DNS update protocol, while TCP ...

#### 6 An analysis of wide-area name server traffic: a study of the Internet Domain Name System



Peter B. Danzig, Katia Obraczka, Anant Kumar

October 1992 **ACM SIGCOMM Computer Communication Review , Conference proceedings on Communications architectures & protocols SIGCOMM '92**, Volume 22 Issue 4

**Publisher:** ACM Press

Full text available: [pdf\(1.19 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Over a million computers implement the Internet's Domain Name System of DNS, making it the world's most distributed database and the Internet's most significant source of wide-area RPC-like traffic. Last year, over eight percent of the packets and four percent of the bytes that traversed the NSFnet were due to DNS. We estimate that a third of this wide-area DNS traffic was destined to seven root name servers. This paper explores the performance of DNS based on two 24-hour t ...

#### 7 IPNL: A NAT-extended internet architecture




Paul Francis Ramakrishna

August 2001 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '01**, Volume 31 Issue 4

**Publisher:** ACM Press

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

Full text available:  [pdf\(241.65 KB\)](#)[terms](#)


This paper presents and analyzes IPNL (for IP Next Layer), a NAT-extended Internet protocol architecture designed to scalably solve the address depletion problem of IPv4. A NAT-extended architecture is one where only hosts and NAT boxes are modified. IPv4 routers and support protocols remain untouched. IPNL attempts to maintain all of the original characteristics of IPv4, most notably address prefix location independence. IPNL provides true site isolation (no renumbering), and allows sites to be ...

## 8 Survey of network-based defense mechanisms countering the DoS and DDoS problems



Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao  
April 2007 **ACM Computing Surveys (CSUR)**, Volume 39 Issue 1

**Publisher:** ACM Press

Full text available:  [pdf\(1.17 MB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

This article presents a survey of denial of service attacks and the methods that have been proposed for defense against these attacks. In this survey, we analyze the design decisions in the Internet that have created the potential for denial of service attacks. We review the state-of-art mechanisms for defending against denial of service attacks, compare the strengths and weaknesses of each proposal, and discuss potential countermeasures against each defense mechanism. We conclude by highlight ...

**Keywords:** Botnet, DDoS, DNS reflector attack, DoS, IP spoofing, IP traceback, IRC, Internet security, SYN flood, VoIP security, bandwidth attack, resource management

## 9 Mobile networking in the Internet

Charles E. Perkins  
December 1998 **Mobile Networks and Applications**, Volume 3 Issue 4

**Publisher:** Kluwer Academic Publishers

Full text available:  [pdf\(166.90 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)


Computers capable of attaching to the Internet from many places are likely to grow in popularity until they dominate the population of the Internet. Consequently, protocol research has shifted into high gear to develop appropriate network protocols for supporting mobility. This introductory article attempts to outline some of the many promising and interesting research directions. The papers in this special issue indicate the diversity of viewpoints within the research community, and it is ...

## 10 Separating key management from file system security



David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel  
December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5

**Publisher:** ACM Press

Full text available:  [pdf\(1.77 MB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)


No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use. We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

11 DNS performance and the effectiveness of caching


Jaeyeon Jung, Emil Sit, Hari Balakrishnan, Robert Morris

October 2002 **IEEE/ACM Transactions on Networking (TON)**, Volume 10 Issue 5**Publisher:** IEEE PressFull text available:  [pdf\(458.33 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

This paper presents a detailed analysis of traces of domain name system (DNS) and associated TCP traffic collected on the Internet links of the MIT Laboratory for Computer Science and the Korea Advanced Institute of Science and Technology (KAIST). The first part of the analysis details how clients at these institutions interact with the wide-area domain name system, focusing on client-perceived performance and the prevalence of failures and errors. The second part evaluates the effectiveness of ...

**Keywords:** DNS, caching, internet, measurement, performance12 Application level performance: DNS performance and the effectiveness of caching Jaeyeon Jung, Emil Sit, Hari Balakrishnan, Robert MorrisNovember 2001 **Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement IMW '01****Publisher:** ACM PressFull text available:  [pdf\(2.84 MB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

This paper presents a detailed analysis of traces of DNS and associated TCP traffic collected on the Internet links of the MIT Laboratory for Computer Science and the Korea Advanced Institute of Science and Technology (KAIST). The first part of the analysis details how clients at these institutions interact with the wide-area DNS system, focusing on performance and prevalence of failures. The second part evaluates the effectiveness of DNS caching. In the most recent MIT trace, 23% of lookups rece ...

13 Stateful distributed interposition John Reumann, Kang G. ShinFebruary 2004 **ACM Transactions on Computer Systems (TOCS)**, Volume 22 Issue 1**Publisher:** ACM PressFull text available:  [pdf\(833.84 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Interposition-based system enhancements for multitiered servers are difficult to build because important system context is typically lost at application and machine boundaries. For example, resource quotas and user identities do not propagate easily between cooperating services that execute on different hosts or that communicate with each other via intermediary services. Application-transparent system enhancement is difficult to achieve when such context information is obscured by complex service ...

**Keywords:** Distributed computing, component services, distributed context, multitiered services, operating systems, server consolidation14 Trust management for IPsec May 2002 **ACM Transactions on Information and System Security (TISSEC)**, Volume 5 Issue 2**Publisher:** ACM PressFull text available:  [pdf\(321.98 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

IPsec is the standard suite of protocols for network-layer confidentiality and authentication of Internet traffic. The IPsec protocols, however, do not address the

policies for how protected traffic should be handled at security end points. This article introduces an efficient policy management scheme for IPsec, based on the principles of trust management. A compliance check is added to the IPsec architecture that tests packet filters proposed when new security associations are created for confo ...

**Keywords:** Credentials, IPsec, KeyNote, network security, policy, trust management

# 15 Development of the domain name system



P. Mockapetris, K. J. Dunlap

August 1988 **ACM SIGCOMM Computer Communication Review, Symposium proceedings on Communications architectures and protocols SIGCOMM '88**, Volume 18 Issue 4

**Publisher:** ACM Press

Full text available: [pdf\(1.24 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The Domain Name System (DNS) provides name service for the DARPA Internet. It is one of the largest name services in operation today, serves a highly diverse community of hosts, users, and networks, and uses a unique combination of hierarchies, caching, and datagram access. This paper examines the ideas behind the initial design of the DNS in 1983, discusses the evolution of these ideas into the current implementations and usages, notes conspicuous surprises, successes and shortc ...

# 16 Development of the Domain Name System



Paul V. Mockapetris, Kevin J. Dunlap

January 1995 **ACM SIGCOMM Computer Communication Review**, Volume 25 Issue 1

**Publisher:** ACM Press

Full text available: [pdf\(983.50 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#)

The Domain Name System (DNS) provides name service for the DARPA Internet. It is one of the largest name services in operation today, serves a highly diverse community of hosts, users, and networks, and uses a unique combination of hierarchies, caching, and datagram access. This paper examines the ideas behind the initial design of the DNS in 1983, discusses the evolution of these ideas into the current implementations and usages, notes conspicuous surprises, successes and shortcomings, and attem ...

# 17 Applications: Inferring relative popularity of internet applications by actively querying



**DNS caches**

Craig E. Wills, Mikhail Mikhailov, Hao Shang

October 2003 **Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement IMC '03**

**Publisher:** ACM Press

Full text available: [pdf\(257.56 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

In this work, we propose a novel methodology that can be used to assess the relative popularity for any Internet application based on the data servers it uses. The basic idea is to infer popularity of data servers by periodically "poking" at local Domain Name servers (LDNSs) that service Domain Name System requests from a set of users running Internet applications and determining if LDNSs have cached resource records for the data servers. This approach allows us to measure the relative percentag ...

**Keywords:** active content measurement, domain name system

# 18 GPRSWeb: optimizing the web for GPRS links



Rajiv Chakravorty, Andrew Clark, Ian Pratt

May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03**

Publisher: ACM Press

Full text available: pdf(1.03 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

The General Packet Radio Service (GPRS) is being deployed by GSM network operators world-wide, and promises to offer users "always-on" data access at bandwidths comparable to that of conventional fixed-line telephone modems. Unfortunately, many users have found the reality to be rather different, experiencing very disappointing performance when, for example, browsing the web over GPRS. In this paper we investigate what causes the HTTP protocol and its underlying transport TCP to underperform in a ...

19 A system for authenticated policy-compliant routing

Barath Raghavan, Alex C. Snoeren

August 2004 **ACM SIGCOMM Computer Communication Review, Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '04**, Volume 34 Issue 4

Publisher: ACM Press

Full text available: pdf(219.77 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Internet end users and ISPs alike have little control over how packets are routed outside of their own AS, restricting their ability to achieve levels of performance, reliability, and utility that might otherwise be attained. While researchers have proposed a number of source-routing techniques to combat this limitation, there has thus far been no way for independent ASes to ensure that such traffic does not circumvent local traffic policies, nor to accurately determine the correct party to char ...

**Keywords:** authentication, capabilities, overlay networks, source routing20 New architectures: Steps towards a DoS-resistant internet architecture

Mark Handley, Adam Greenhalgh

August 2004 **Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture FDNA '04**

Publisher: ACM Press

Full text available: pdf(120.88 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Defending against DoS attacks is extremely difficult; effective solutions probably require significant changes to the Internet architecture. We present a series of architectural changes aimed at preventing most flooding DoS attacks, and making the remaining attacks easier to defend against. The goal is to stimulate a debate on trade-offs between the flexibility needed for future Internet evolution and the need to be robust to attack.

**Keywords:** denial-of-service, internet, network architecture, security

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	(IPSEC protocol security domain resolution processor cache).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/06/10 14:32
L6	1	(IPSEC protocol processing resolution cache).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/06/10 14:37
L8	0	(IPSEC protocol execution resolution cache).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/06/10 14:37
L12	0	(secure domain name resolution IPSEC cache security policy DNS identifying).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/06/10 14:39

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	731	(713/170).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/06/10 14:49
L2	3071	((726/3) or (726/4) or (726/5) or (726/6)).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/06/10 14:50
L3	3748	L2 or L1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 14:50
L4	55	L3 and (IPSEC and cache)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 14:50
L5	13	L4 and @ad<"20010608"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 14:52
L6	284	(IPSEC and cache and entries and domain and resolution)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 14:52
L7	99	L6 and @ad<"20010608"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 14:52
L8	7	(IPSEC same cache same (domain adj name))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 14:53
L9	0	L8 and @ad<"20010608"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 14:53



## EAST Search History

L10	48	IPSEC and (cache same (domain adj name))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 14:53
L11	8	L10 and @ad<"20010608"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 15:02
L12	11	(Internet adj Protocol adj Security) and (cache same (domain adj name))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 15:01
L13	0	L12 and @ad<"20010608"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 15:03
L14	71	(IPSEC and cache and (domain adj name) and (security adj policy) and server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 15:04
L15	14	L14 and @ad<"20010608"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 15:04
L17	31	(IPSEC and cache and (domain adj name) and (security adj policy) and server and (IP with layer))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 15:05
L18	14	L17 and @ad<"20010608"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 15:06
L19	22	(IPSEC and cache and (domain adj name) and (security adj policy) and (DNS with server) and (IP with layer))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 15:05

## EAST Search History

L20	11	L19 and @ad<"20010608"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/10 15:08
L22	13	(TROSTLE JONATHAN).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/06/10 15:10
L23	16	(GOSSMAN WILLIAM).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/06/10 15:11